Amazon Web Services, Inc.

AWS Scalable Network Crypto Modules, version 1.1

Version: 1.0

FIPS 140-3 Non-Proprietary Security Policy

Document prepared by:

http://www.lightshipsec.com

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This non-proprietary FIPS 140-3 Security Policy for the AWS Scalable Network Crypto Modules, version 1.1 describes how the module meets the security requirements specified in FIPS 140-3 for an overall security level 1 module and outlines the security rules and operating procedures required to maintain compliance.

1.2 Security Levels

Section	Title	Security Level
1	General	1
2	Cryptographic module specification	1
3	Cryptographic module interfaces	1
4	Roles, services, and authentication	1
5	Software/Firmware security	1
6	Operational environment	1
7	Physical security	1
8	Non-invasive security	N/A
9	Sensitive security parameter management	1
10	Self-tests	1
11	Life-cycle assurance	1
12	Mitigation of other attacks	N/A
	Overall Level	1

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

MACsec and DWDM link encryption is used by AWS networking infrastructure to secure traffic across its core network consisting of long-distance and large-scale data communications across the globe. Traffic flowing across the AWS global network is protected by strong cryptography and meets regulatory requirements.

Module Type: Software-hybrid

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:

The cryptographic boundary of the AWS Scalable Network Crypto Module consists of a hardware and a software component, which is represented by the red dash line in Figure 4, below. The software components of the module consist of the *IV Helper*, *Self-test & Error Manager,* and a pre-loaded HMAC digest for integrity testing. The Acacia AC1200 (with Pico DSP) (figures 1 and 2) and Acacia AX1200 (with Jannu DSP) (figure 3), are pictured below. The chips represent the physical perimeter of the modules and implement the core

cryptographic functionality, AES-GCM encryption and decryption used within the MACsec protocol. They install in the pluggable sled slots on the front of the AZ3324 & CS8320. Up to four iterations of the AWS Scalable Encryption Module can be installed in the AZ3324 & CS8320 chassis at any given point in time. The modules operate separately from each other and only share access to the AWS-LC library as shown in Figure 4.

Tested Operational Environment's Physical Perimeter (TOEPP):

The tested operational environment's physical perimeter is defined as the AWS Network devices (AZ3324 & CS8320) that contain the module. The TOEPP is represented in Figure 4, and depicted in Figures 5 and 6, below.

Figure 1: Acacia AC1200 pluggable encryptor unit

Figure 2: Acacia Pico DSP (housed inside AC1200)

Figure 3: Acacia AX1200 (with Jannu DSP) physical perimeter

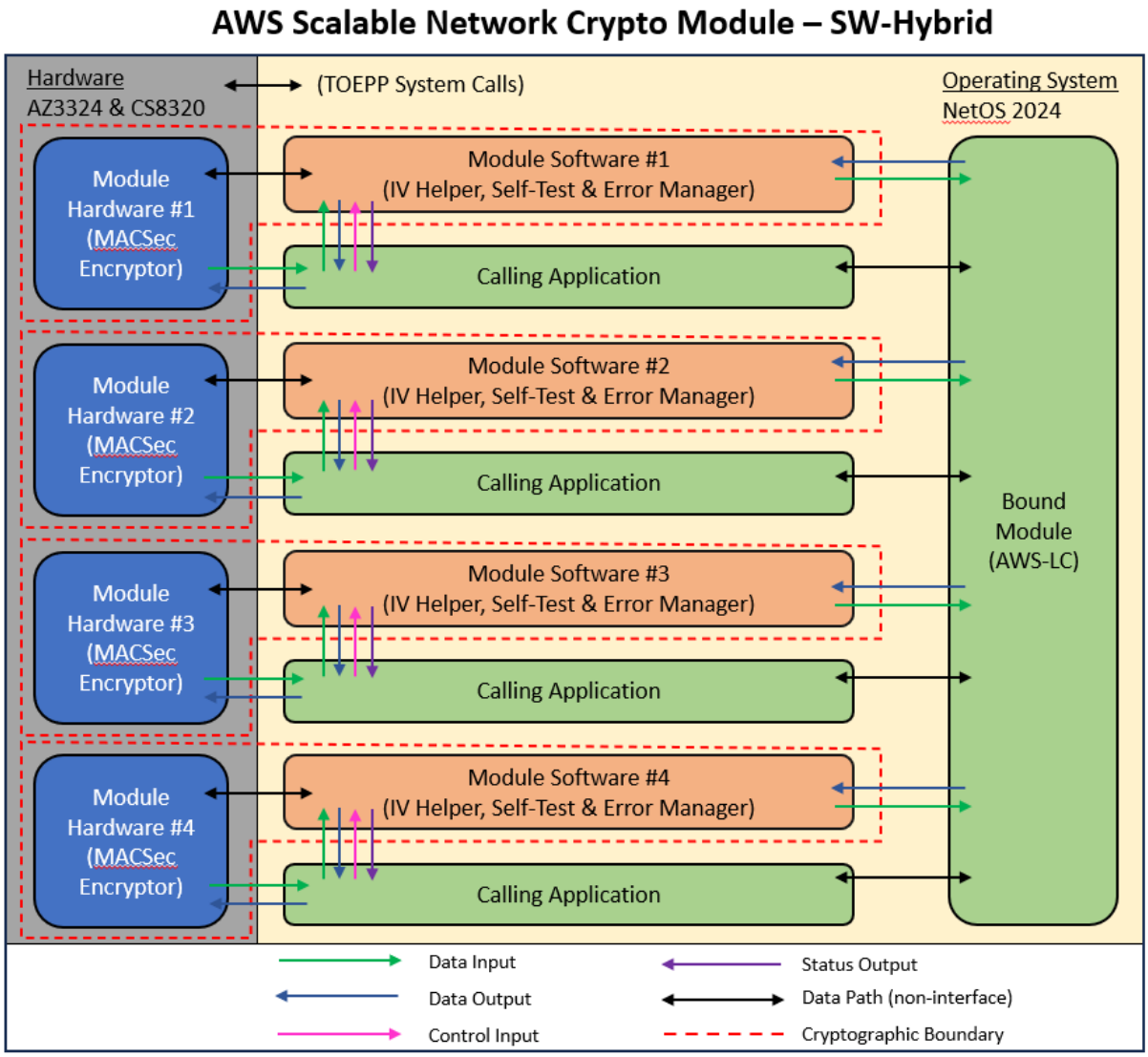

Figure 4: Block diagram and module cryptographic boundary

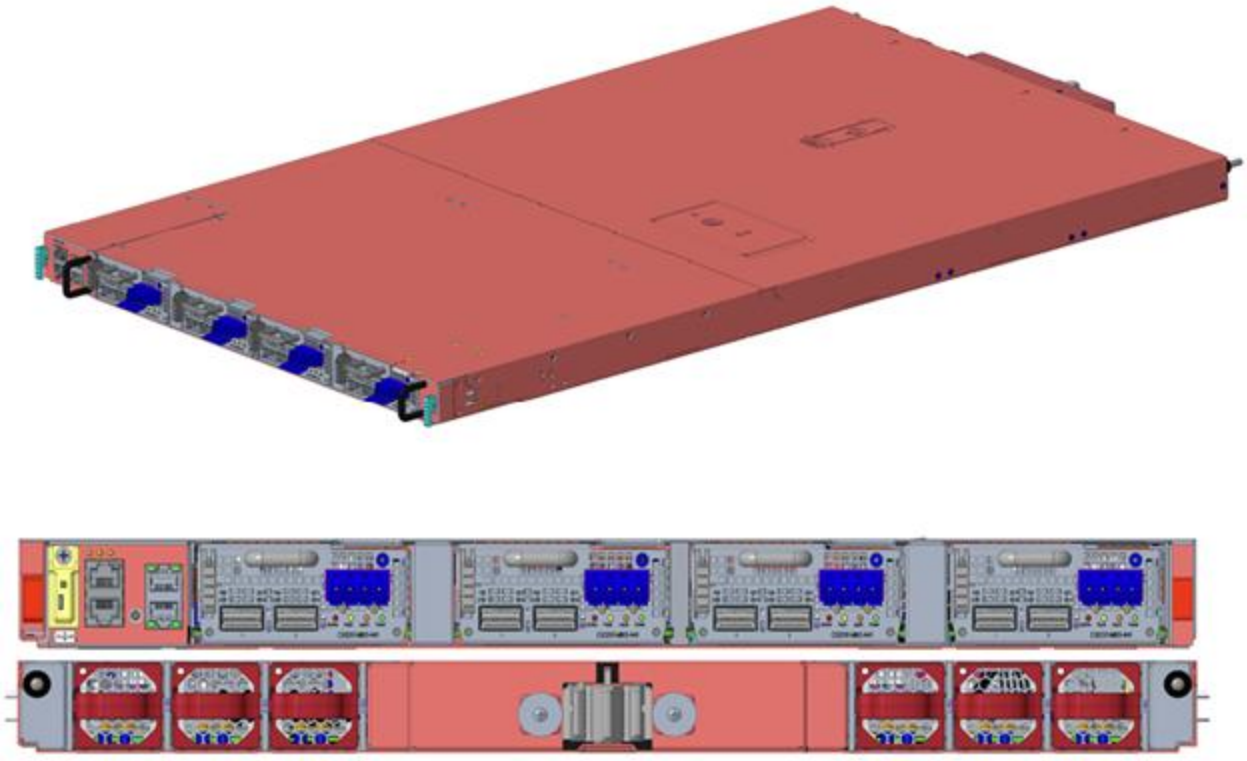

Figure 5: The AZ3324 device chassis containing 4 AX1200 units

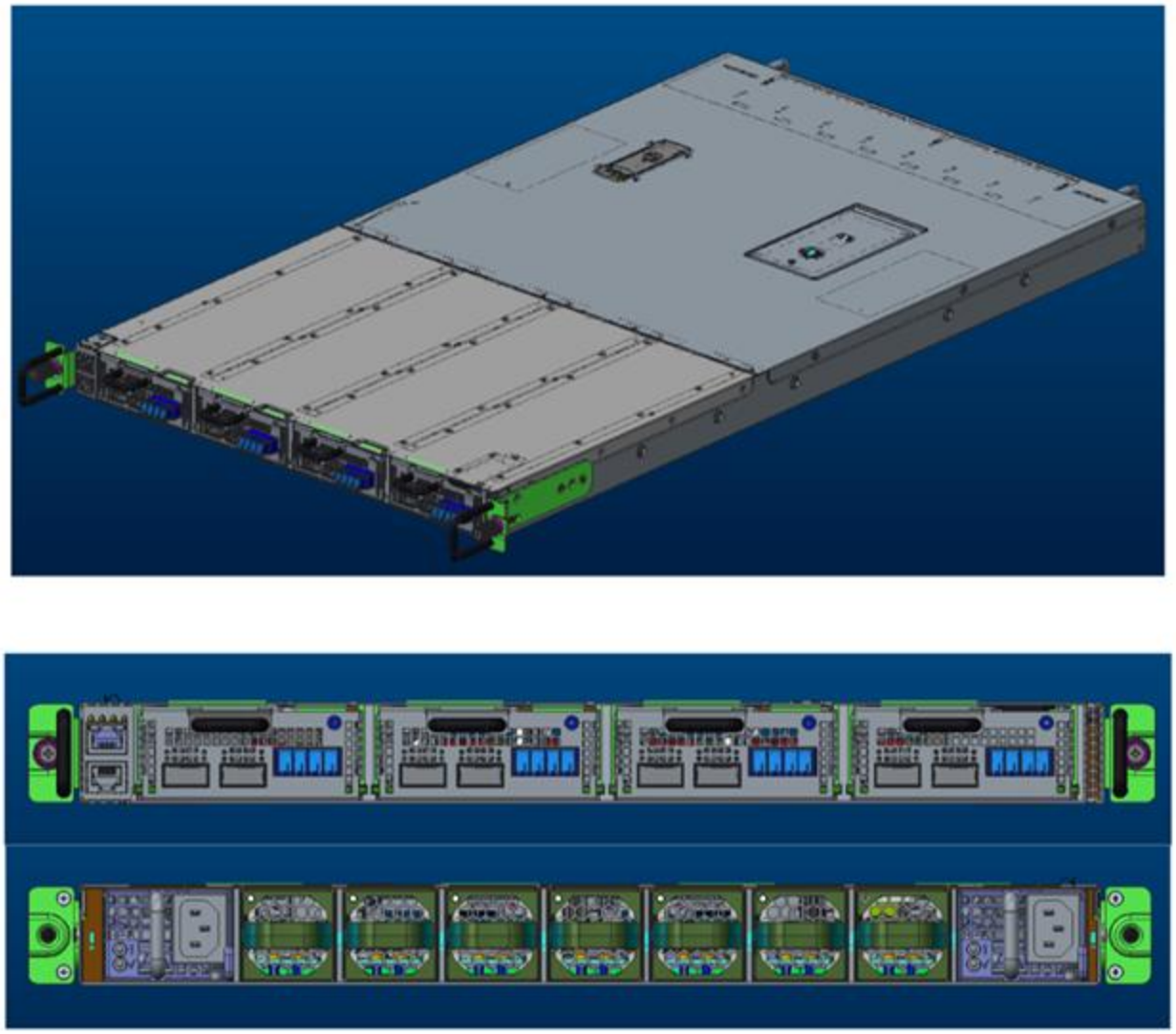

Figure 6: The CS8320 device chassis containing 4 AC1200 units

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

Package or File Name	Software/ Firmware Version	Features	Integrity Test
NetOS-MACSec-Self-Tests	1.1	Contains GCM IV Helper, Self-Test & Error Manager, HMAC file	HMAC-SHA2-256

Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)

Tested Module Identification – Hybrid Disjoint Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
Acacia AC1200	AC1200-MN3-440	1.0	Pico DSP	Housed in pluggable unit with optical ports
Acacia AX1200	AX1200-8X9-44C	1.0	Jannu DSP	Housed in pluggable unit with optical ports

Table 3: Tested Module Identification – Hybrid Disjoint Hardware

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
NetOS 2024	CS8320	Annapurna K2X-N (arm64)	Yes	-	1.1
NetOS 2024	AZ3324	NXP Layerscape LX2080 (arm64)	Yes	-	1.1

Table 4: Tested Operational Environments - Software, Firmware, Hybrid

2.3 Excluded Components

There are no module components excluded from the validation.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved mode	The approved mode of operation	Approved	syslog (code=exited, status=0/SUCCESS)

Table 5: Modes List and Description

When the module is powered up, the integrity of the module software is checked using an approved software integrity check mechanism (HMAC-SHA2-256), by the bound module ("AWS-LC Cryptographic Module (dynamic build)", version "AWS-LC FIPS 1.29.0"). Once these self-tests have completed successfully, the module transitions into the approved mode of operation. There are no other modes of operation implanted by the module.

2.5 Algorithms

Approved Algorithms:

AZ3324 device with AX1200 encryptor

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	A4847	Direction - Encrypt Key Length - 256	SP 800-38A
AES-GCM	A4847	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 256	SP 800-38D

Table 6: Approved Algorithms - AZ3324 device with AX1200 encryptor

CS8320 device with AC1200 encryptor

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	C373	Direction - Encrypt Key Length - 256	SP 800-38A
AES-GCM	C681	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 256	SP 800-38D

Table 7: Approved Algorithms - CS8320 device with AC1200 encryptor

[EVM] AWC-LC (Integrity Test)

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-256	A5425	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A5433	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A5434	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
SHA2-256	A5425	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A5433	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A5434	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4

Table 8: Approved Algorithms - [EVM] AWC-LC (Integrity Test)

The Approved Algorithms tables above list the approved algorithms implemented by the AWS Encryption Module and the algorithms implemented within the bound module, which are used to perform the software integrity test upon the module.

Vendor-Affirmed Algorithms:

The module does not implement any vendor-affirmed algorithms.

Non-Approved, Allowed Algorithms:

The module does not implement any non-approved, allowed algorithms.

Non-Approved, Allowed Algorithms with No Security Claimed:

The module does not implement any non-approved, allowed algorithms with no security claimed.

Non-Approved, Not Allowed Algorithms:

The module does not implement any non-approved, not allowed algorithms.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Encrypt Data	BC-Auth	Encryption of data in MACsec protocol	Publication:NIST SP 800-38D IG:C.H	AES-GCM: (C681, A4847) AES-ECB: (C373, A4847)
Decrypt Data	BC-Auth	Encryption of data in MACsec protocol	Publication:NIST SP 800-38D IG:C.H	AES-GCM: (C681, A4847) AES-ECB: (C373, A4847)
Software Integrity Test	MAC	[EVM] Integrity check using HMAC-SHA2-256 implemented in AWS-LC (bound module)		HMAC-SHA2-256: (A5425, A5433, A5434) SHA2-256: (A5425, A5433, A5434)

Table 9: Security Function Implementations

2.7 Algorithm Specific Information

The AES-GCM Initialization Vector (IV) generation is compliant with IG C.H, resolution 1(c). The module generates IVs deterministically following the guidance in IEEE 802.1AE.

While operating the approved mode of operation, the module should only be used to form a MACsec link with another FIPS 140 validated module operating in the approved mode. The device on each end of the MACsec link plays the role of either the Peer or the Authenticator. No authentication server is involved.

As required by the MACsec module (IEEE 802.1AE), the IV has a length of 96 bits and is constructed by the “IV Helper” by concatenating the 64-bit Secure Channel Identifier (SCI) with the 32-bit Packet Number (PN)

In case the module’s power is lost and then restored, the key used for AES-GCM encryption and decryption operations shall be redistributed.

2.8 RBG and Entropy

The module only generates SSPs used in the MACsec protocol deterministically. Therefore, the module does not implement a DRBG and does not require an entropy source.

2.9 Key Generation

The module only generates AES-GCM IVs deterministically per the guidance given in IG C.H and IEEE 802.1AE.

2.10 Key Establishment

The module does not implement any key establishment schemes.

2.11 Industry Protocols

The module is an encryption component and does not implement any industry protocols.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
(AC1200) PCIE_TDP, PCIE_TDN, PCIE_RDP, PCIE_RDN, PCIE_REFCLK_P, PCIE_REFCLK_N; (AX1200) TX0-15P/N, Duplex Connector	Data Input	Plaintext data to be encrypted, Encrypted data to be decrypted
(AC1200) PCIE_TDP, PCIE_TDN, PCIE_RDP, PCIE_RDN, PCIE_REFCLK_P, PCIE_REFCLK_N; (AX1200) RX0-15P/N, Duplex Connector	Data Output	Plaintext data that has been decrypted, Encrypted data that has been encrypted
(AC1200) PCIE_TDP, PCIE_TDN, PCIE_RDP, PCIE_RDN, PCIE_REFCLK_P, PCIE_REFCLK_N; (AX1200) TX0-15P/N	Control Input	Function calls from the calling applications
(AC1200) PCIE_TDP, PCIE_TDN, PCIE_RDP, PCIE_RDN, PCIE_REFCLK_P, PCIE_REFCLK_N; (AX1200) RX0-15P/N	Status Output	Status information regarding module and services to OS and Calling applications
(AC1200) Voltage_1.8V; (AX1200) Voltage_1.8V	Power	Electrical power to the module

Table 10: Ports and Interfaces

The Ports and Interfaces table above specifies the cryptographic module interfaces. The physical interfaces are defined as the RX/TX or PCIe pins of the encryptor units. The logical interfaces are logically separated from one another by the module's hybrid-software design. The power interface is physically separate from the other physical interfaces as the voltage pins are distinct from the RX/TX/PCIe of the encryptor units. A control output interface is not implemented.

4 Roles, Services, and Authentication

4.1 Authentication Methods

The module does not implement any authentication mechanisms. The sole role (Crypto Officer) is assumed implicitly.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	None

Table 11: Roles

The module supports the Crypto Officer role only. This sole role is implicitly assumed by the operator of the module when performing a service.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show Status	Output approved mode status	Global (completion of service)	Command	Status Output (status=0/SUCCESS, or status=1/FAILURE)	None	Crypto Officer
Show Module's Versioning Information	Output the module name and version identifiers	Global (completion of service)	Command	Status Output (AWS Encryption Module, version 1.1)	None	Crypto Officer
Perform Zeroisation	Zeroise SSPs stored temporarily in RAM	Global (completion of service)	Procedure: Disable individual encryptor, Reboot host device	Status Output: "Sled <#> disabled successfully", Module reboot	None	Crypto Officer - AES-GCM Key: Z - AES-GCM IV: Z
Perform Self-Tests	Perform the module's cryptographic self-tests on demand	Global (completion of service)	Procedure: Enable individual encryptor, Reboot host device	Status Output: "(code=exited, status=0/SUCCESS)"	None	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
[EVM] Perform Self-tests	Perform the EVM's CASTs, and the Integrity Check upon the module	Global (completion of service)	Procedure: Enable individual encryptor, Reboot host device	Status Output: "(code=exited, status=0/SUCCESS)"	Software Integrity Test	Crypto Officer
Encrypt Data	Encrypt plaintext data	Global (completion of service)	Plaintext Data (Network Traffic)	Encrypted Data (Network Traffic)	Encrypt Data	Crypto Officer - AES-GCM Key: E - AES-GCM IV: G,E
Decrypt Data	Decrypt ciphertext data	Global (completion of service)	Encrypted Data (Network Traffic)	Plaintext Data (Network Traffic)	Decrypt Data	Crypto Officer - AES-GCM Key: E - AES-GCM IV: E

Table 12: Approved Services

The module provides approved services to the operator who assumes the Crypto Officer role as defined in this document. The approved services defined in this section implement the security function implementations defined in section 2.6 of this document.

The Crypto Officer can confirm that they are operating the “AWS Scalable Network Crypto Modules, version 1.1” module by checking for the output “AWS Encryption Module, version 1.1” from the module’s *Show Module's Versioning Information* service.

4.4 Non-Approved Services

The module does not implement any non-approved services.

4.5 External Software/Firmware Loaded

The module does not allow the loading of external software or firmware.

5 Software/Firmware Security

5.1 Integrity Techniques

The module's software integrity self-test is managed within the module boundary by the *Self-Test and Error Manager*, which calls the function fips_helper.py. During the module's pre-operational self-tests, the self-test and error handler passes the stored HMAC-SHA2-256 digest to the bound module (AWS-LC FIPS 1.29.0) to which calculates the HMAC of the module software package and passes the result back to the Self-test and error handler. The *Self-Test and Error Manager* compares the result with the stored HMAC file. If the 2 HMAC values do not match, the integrity test fails, and the module enters the error state.

The bound module (AWS-LC FIPS 1.29.0) must have passed its own software integrity test and HMAC-SHA2-256 CAST before performing the HMAC calculation of the AWS Encryption module's software.

5.2 Initiate on Demand

The conditional algorithm self-tests are run at module startup in addition to the software integrity test. The crypto officer can initiate the self-tests on demand for the module by entering the command "sledcmd --sled <#> enable", or for all module's present within the TOEPP by power-cycling the host device.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

The operating environments for the module are the AWS CS8320 and AZ3324 network devices running NetOS 2024, which are limited operational environments. The module operational environments are physically housed within a secure AWS facility and come pre-configured in the approved mode by AWS engineers. AWS customers purchase infrastructure as-a-service and have no direct system-level access to the host device.

The Crypto Officer should confirm that the module is operating in the approved mode by checking for the approved mode indicator per the instructions in Section 11.2 of this document.

7 Physical Security

Each module's hardware consists of a the pluggable encryptor units which are made using production grade components. The encryptor units house the DSP chips, which consist of production grade components protected by a conformal coating as a standard passivation technique. As the software portion of the hybrid module execute within a limited operational environment, the module is defined as a multi-chip standalone embodiment.

The module itself provides no additional physical security techniques. However, the module will reside inside of an AWS device which is installed within a secure AWS facility. The module will therefore inherit these additional physical characteristics and protections.

8 Non-Invasive Security

The module does not implement any security mechanisms which protect against non-invasive attacks.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Volatile Memory	Process space of 'FIPS Helper', Chips registers	Dynamic
External	Process space of the calling applications	Dynamic

Table 13: Storage Areas

The module stores keys and input/output data temporarily in volatile memory. The module does not store keys or data persistently.

9.2 SSP Input-Output Methods

N/A for this module.

SSPs are only input from or output to the calling applications within the module's TOEPP. This method is categorized as manual distribution, electronic entry/output ("CM Software to/from App via TOEPP Path").

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Remove Power	Remove power from the host platform	Keys are procedurally zeroized by rebooting the host platform, which is acceptable at Software level 1.	Crypto Officer reboots or removed power from host platform
Disable/remove SLED	Remove individual pluggable encryptor unit	Keys are procedurally zeroized by removing the individual encryptor unit, thus removing power, which is acceptable at Software level 1.	Crypto Officer removes SLED (pluggable encryptor) from host platform

Table 14: SSP Zeroization Methods

SSPs are zeroised procedurally by power-cycling the host platform.

9.4 SSPs

The following table summarizes the Sensitive Security Parameters (SSPs) that are used by the cryptographic services implemented:

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES-GCM Key	Encryption and Decryption	256 bits - 256 bits	Authenticated Symmetric Key - CSP	Encrypt Data Decrypt Data		Encrypt Data Decrypt Data
AES-GCM IV	Initialization Vector for AES-GCM MACsec encryption	96 bits - N/A	Keying Material - PSP	Encrypt Data Decrypt Data		Encrypt Data Decrypt Data

Table 15: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES-GCM Key		Volatile Memory:Plaintext	Until zeroised	Remove Power	AES-GCM IV:Used With
AES-GCM IV		Volatile Memory:Plaintext	Until zeroised	Remove Power	AES-GCM Key:Used With

Table 16: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-256 (A5425)	SHA2-256	KAT	SW/FW Integrity	syslog entry	[EVM] Calculate hash of entire module software and compare to known answer
HMAC-SHA2-256 (A5433)	SHA2-256	KAT	SW/FW Integrity	syslog entry	[EVM] Calculate hash of entire module software and compare to known answer
HMAC-SHA2-256 (A5434)	SHA2-256	KAT	SW/FW Integrity	syslog entry	[EVM] Calculate hash of entire module software and compare to known answer

Table 17: Pre-Operational Self-Tests

The module's startup integrity test is performed upon the module's software by the bound module (Amazon's AWS-LC Cryptographic module).

As the modules do not implement bypass capability or any FIPS-defined critical functions, no additional pre-operational self-tests are required.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (C681)	256 bits	KAT	CAST	syslog entry ("encryption test passed" / "encryption test failure")	Encrypt	Before first operational use of AES-GCM / Immediately when the module enters the approved mode of operation
AES-GCM Decrypt (C681)	256 bits	KAT	CAST	syslog entry ("decryption test passed" / "decryption test failure")	Decrypt	Before first operational use of AES-GCM / Immediately when the module enters the approved mode of operation

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A4847)	256 bits	KAT	CAST	syslog entry ("encryption test passed" / "encryption test failure")	Encrypt	Before first operational use of AES-GCM / Immediately when the module enters the approved mode of operation
AES-GCM Decrypt (A4847)	256 bits	KAT	CAST	syslog entry ("decryption test passed" / "decryption test failure")	Decrypt	Before first operational use of AES-GCM / Immediately when the module enters the approved mode of operation
HMAC-SHA2-256 (A5425)	SHA2-256	KAT	CAST	syslog entry	[EVM] CAST performed by the bound module on it's own HMAC-SHA implementation before running Integrity Test on itself or the module	[EVM] Before first operational use of bound module integrity test / Immediately when the module enters the approved mode of operation
HMAC-SHA2-256 (A5433)	SHA2-256	KAT	CAST	syslog entry	[EVM] CAST performed by the bound module on it's own HMAC-SHA implementation before running Integrity Test on itself or the module	[EVM] Before first operational use of bound module integrity test / Immediately when the module enters the approved mode of operation

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-256 (A5434)	SHA2-256	KAT	CAST	syslog entry	[EVM] CAST performed by the bound module on it's own HMAC-SHA implementation before running Integrity Test on itself or the module	[EVM] Before first operational use of bound module integrity test / Immediately when the module enters the approved mode of operation

Table 18: Conditional Self-Tests

The conditional self-test for AES-GCM is run at module instantiation, before the first operational use of the algorithm. The underling AES-ECB algorithm's self-test requirements are satisfied by the running of the AES-GCM self-test per IG 10.3.A, Resolution 1.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A5425)	KAT	SW/FW Integrity	Upon module startup	Manual (reboot host platform)
HMAC-SHA2-256 (A5433)	KAT	SW/FW Integrity	Upon module startup	Manual (reboot host platform)
HMAC-SHA2-256 (A5434)	KAT	SW/FW Integrity	Upon module startup	Manual (reboot host platform)

Table 19: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (C681)	KAT	CAST	On Demand / On Startup	Manually
AES-GCM Decrypt (C681)	KAT	CAST	On Demand / On Startup	Manually
AES-GCM (A4847)	KAT	CAST	On Demand / On Startup	Manually
AES-GCM Decrypt (A4847)	KAT	CAST	On Demand / On Startup	Manually
HMAC-SHA2-256 (A5425)	KAT	CAST	On Demand / On Startup	Manually
HMAC-SHA2-256 (A5433)	KAT	CAST	On Demand / On Startup	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A5434)	KAT	CAST	On Demand / On Startup	Manually

Table 20: Conditional Periodic Information

The operator can perform the pre-operational and conditional self-tests on demand by re-instantiating the individual module or power-cycling the host device.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error	Hard Error State: MACsec interfaces do not come up	Module fails any self-test	Replace pluggable unit and re-instantiate module / reboot host platform	syslog entry (status=1/FAILURE)

Table 21: Error States

When the module fails any self-test, the module will immediately print a self-test failure indicator to the syslog. The identified failure indicator for the module integrity test is “SELF TEST FAILED!!!. Reason - Integrity tests failed”. The identified failure indicator for the AES-GCM CAST is “self test failed on sled - <#>”. The module will automatically perform zeroisation of all SSPs within the module boundary and transition to the Error state, printing an error state indicator to the syslog (*code=exited, status=1/FAILURE*). When in the error state, the failed encryptor’s interfaces will not be available and therefore, all cryptographic operation is inhibited.

10.5 Operator Initiation of Self-Tests

The operator can perform the pre-operational and conditional self-tests on demand by re-instantiating the individual module. The operator can also perform pre-operational and conditional self-tests for all modules within the TOEPP by rebooting the host device.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The AWS Encryption Module is pre-installed and configured at an AWS facility and offered to end users as an integrated part of AWS' service offerings. As such, there are no installation, initialization, or startup procedures to be performed by the Crypto Officer.

11.2 Administrator Guidance

The Crypto Officer should ensure that the module is running in the approved mode of operation before use. This can be determined by checking the syslog for the approved mode indicator (*code=exited, status=0/SUCCESS*).

If an individual instance of the module has entered the error mode by failing any self-test, the module can be replaced by the crypto officer by performing the following steps:

1. Disable the failed module by entering "sledcmd --sled <#> disable"
2. Disconnect and replace the pluggable encryptor unit
3. Instantiate the module instance for the new encryptor by entering "sledcmd –sled <#> enable"

If the TOEPP has less than 4 encryptor units active, the Crypto Officer may add additional encryptors by performing the following steps:

1. Connect the pluggable encryptor unit to an empty SLED bay
2. Instantiate the module instance for the new encryptor by entering "sledcmd –sled <#> enable"

Either of the above processes will create a new instance of the module software and calling application (outside of boundary) to manage the new encryptor unit. The module will automatically perform its initialization routine including the running of all pre-operational and conditional self-tests.

11.3 Non-Administrator Guidance

In case the module's power is lost and then restored, the key used for MACsec encryption and decryption shall be redistributed.

12 Mitigation of Other Attacks

The module does not implement any security mechanisms which protect against other attacks.